УДК 004.422.8+004.738.56.5+342.2/7 : 004.056

Гузенкова Е. А.

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ РЕАЛИЗАЦИИ ОБЛАЧНЫХ ТЕХНОЛОГИЙ ДЛЯ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Рассматриваются облачные сервисы, необходимые для удаленного выполнения работ по дисциплинам студентами и обеспечении информационной безопасности облачной среды виртуализации и хранения информации в облаке.В статье приведены преимущества применения облачных технологий на базе платформ VMwarevSphere с обработкой данных ограниченного доступа в виртуальной среде – vGate. Данное решение обеспечивает защиту средств управления виртуальной инфраструктурой и обладает функционаломмандатного и дискреционного разграничения доступа к объектам, которые размещены внутри защищаемого периметра.Сервер авторизации vGate защищает периметр сети администрирования и разграничивает доступ серверам виртуализации и к средствам управления виртуальной инфраструктуры, а также обладает многими средствами защиты информации, при работе с ней в облачных технологиях, что позволяет реализовывать лабораторные работы на базе частного облака университета.

Ключевые слова: *облачные сервисы, виртуализация рабочих мест, частное облако, средства защиты*

Guzenkova E. A.

PROVIDING INFORMATION SECURITY CLOUD IN THE IMPLEMENTATION OF TECHNOLOGIES TO EDUCATIONAL PROCESS

Cloud services are considered necessary for the remote execution of works by students in the disciplines of information security and cloud virtualization and data storage in the cloud. The

article presents the advantages of using cloud-based platforms with VMware vSphere data processing restricted in a virtual environment - vGate. The solution protects virtual infrastructure management tools and has a functional mandate and discretionary access control to the objects that are placed inside the protected perimeter. The authorization server protects the network perimeter vGate administration and delineates the access server virtualization and virtual infrastructure management tools, and has many means of information protection, while working with her in the cloud technology, which allows to realize laboratory works on the basis of a private cloud University.

Keywords: *cloud computing, desktop virtualization, private cloud, remedies*

В современном мире, все большее распространение получают облачные вычисления. За последние годы концепция облачных вычислений стала более востребована, в том числе как платформа для поддержки образовательной деятельности[1].

Сегодня под облачными вычислениями обычно понимают возможность получения необходимых вычислительных мощностей по запросу из сети.

С ростом числа часов самостоятельного изучения дисциплин, становиться актуальным перенос части лабораторного практикума из аудиторного фонда университета, на внеклассное изучение предмета студентами. Основная проблема заключается в том, что оборудование, которым обладает студен, может обладать не достаточной мощностью, для осуществления лабораторного практикума, а также не иметь лицензий на программное обеспечение.

Для большей вовлеченности учащегося в процесс обучения можно реализовать групповую работу над заданиями с помощью удаленного доступа.

Не смотря на привлекательность создания виртуальных рабочего пространства или хранения информации на основе облачных технологий, у них имеется ряд минусов, которые до сих пор являются тормозящим фактором для повсеместного применения данной инфраструктуры в России.

Один из них заключается в необходимости постоянного соединения с сетью Интернет с большой пропускной способностью, то есть скорость работы облачной площадки будет зависеть от пропускной способности канала, и если она не велика, то программное обсечение может работать с большой задержкой по сравнению с локально установленным ПО.

Другим недостатком является то, что при использовании сторонних облачных технологий возникает зависимость он надежности их оборудования, что может привезти к угрозе безопасности как бесперебойной работе, так и к хранимым в облаке данным.

Еще одной угрозой безопасности является доступ к информации, ограниченного доступа. Не все данные можно доверить стороннему провайдеру в интернете, особенно не только для хранения, но и для обработки. Так же при применении виртуальной площадки для выполнения лабораторного практикума возникает опасность доступа сторонних лиц к персональным данным обучающихся и интеллектуальному труду разработчика методических рекомендаций для проведения работ [2].

Что бы решить большинство вышеперечисленных проблем образовательное учреждение может создать на базе своего оборудования приватное частное облако для организации с применением сертифицированного средства защиты информации от несанкционированного доступа и контроля выполнения ИБ-политик для виртуальной инфраструктуры на базе систем VMwarevSphere [3]. А в качестве средства защиты информации для виртуальных инфраструктур применить сертифицированное средство, предназначенное для обеспечения безопасности виртуальных инфраструктур на базе платформ VMwarevSphere 4 и 5 применение, которого дает возможность легитимной обработки данных ограниченного доступа в виртуальной среде – vGate. Имеющее сертификат ФСТЭК России № 2308 от 28 марта 2011 года, действительный до 28 марта 2017года, подтверждающий соответствие vGate требованиям руководящих документов в части защиты от несанкционированного доступа -по 5 классу защищенности (СВТ5) и контроля отсутствия недекларированных возможностей-по 4 уровню контроля (НДВ4), а также может использоваться в АС до класса защищенности 1Г включительно и для защиты информации в ИСПДн до 1 класса включительно.

При развертывании vGate потребуется выделить только один новый сервер для установки сервера авторизации и, возможно, предусмотреть рабочее место для администратора информационной безопасности. Все остальные компоненты vGate развертываются на базе существующего оборудования виртуальной инфраструктуры (рабочие места АВИ и ESX-серверы). АрхитеркурavGate показана на рис. 1.

В vGate реализована модель разделения прав на управление виртуальной инфраструктурой и на управление безопасностью. Таким образом, выделяются две основные роли – это администратор виртуальной инфраструктуры (АВИ) и администратор информационной безопасности (АИБ).

Доступ на управление виртуальной инфраструктурой или параметрами безопасности предоставляется только аутентифицированным пользователям. Причем процедура аутентификации пользователей и компьютеров (рабочих мест АИБ и АВИ) осуществляется по протоколам, нечувствительным к попыткам перехвата паролей и атакам типа ManintheMiddle.

Процедура аутентификации АВИ осуществляется с помощью отдельного приложения, которое устанавливается на его рабочее место (агент аутентификации). До соединения с виртуальной инфраструктурой АВИ требуется запустить эту программу и ввести учетные данные.

Для избавления пользователя от многократного ввода имени пользователя и пароля агент аутентификации включает функцию надежного сохранения учетных данных. Эта функция особенно полезна, когда на рабочем месте администратора установлены несколько систем защиты, каждая из которых запрашивает данные для аутентификации.

Для обеспечения защиты средств управления виртуальной инфраструктурой применяется функционал дискреционного разграничения доступа к объектам, которые размещены внутри защищаемого периметра. Правила разграничения доступа работают на основе заданных ACL и параметров соединения (протоколов, портов). Также в vGate при разграничении прав доступа администраторов виртуальной инфраструктуры к объектам инфраструктуры используется мандатный принцип контроля доступа. Сетевой трафик между аутентифицированными субъектами и защищаемыми объектами подписывается, тем самым обеспечивается защита от атак типа ManintheMiddle в процессе сетевого взаимодействия.

В vGate механизм блокирования любого сетевого трафика со стороны виртуальных машин к средствам управления виртуальной инфраструктурой. Тем самым обеспечивается защита средств управления виртуальной инфраструктурой от НСД со стороны скомпрометированной виртуальной машины.

Так же с помощью данного программного продукта можно обеспечить контроль целостности настроек виртуальных машин перед их загрузкой. Контроль осуществляется

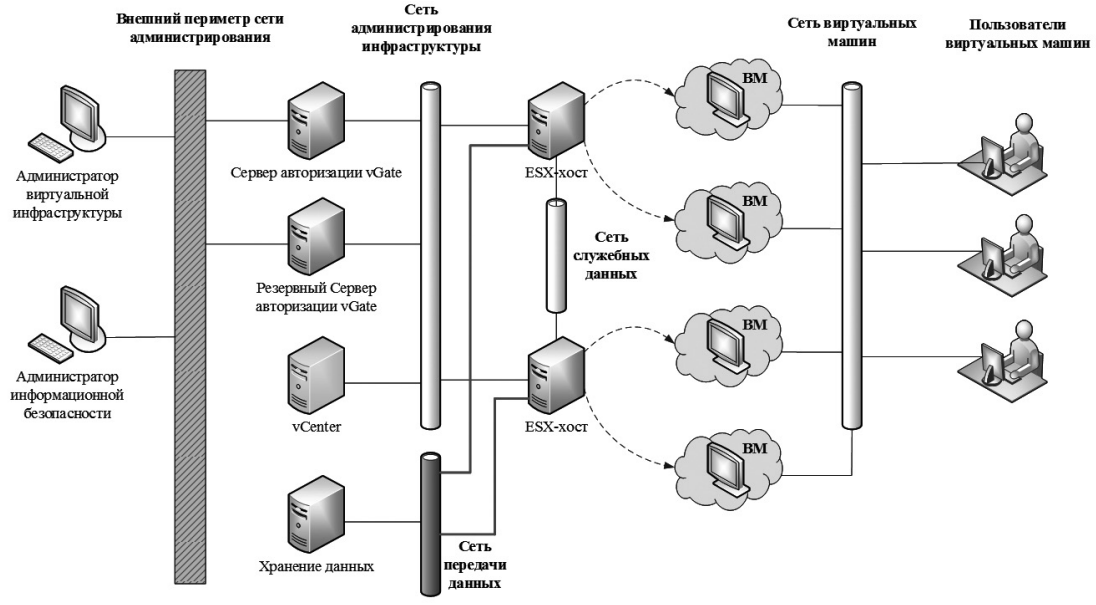

Рис. 1. Архитектура безопасной виртуализации vGate

над файлом *.vmx, в котором содержится перечень устройств, доступных виртуальной машине, и ряд других критических параметров.

По мимо этого осуществляется контроль образа BIOS виртуальной машины. Поскольку несанкционированная подмена BIOS является угрозой безопасности, СЗИ контролирует целостность файла *.nvram, в котором содержится образ BIOS виртуальной машины.

Доверенная загрузка ОС осуществляется путем контроля целостности загрузочного сектора виртуального диска *.vmdk.

При работе в незащищенной виртуальной инфраструктуре на базе систем VMware, администратор этой инфраструктуры обычно может получить доступ к файлам виртуальных машин. Администратор может прямо из VI клиента скачать файл виртуальной машины на локальный диск своего компьютера и исследовать его содержимое. В vGate реализованы механизм, позволяющий этот доступ ограничить.

Консоль управления, входящая в состав СЗИ, устанавливается на рабочее место администратора информационной безопасности и позволяет осуществлять мониторинг системы, управлять правами доступа к защищаемым объектам, управлять параметрами виртуальных машин и осуществлять иные функции, связанные с безопасностью системы.

Все изменения, произведенные администратором информационной безопасности, сохраняются централизованно на сервере авторизации.

На рисунке 1 предусмотрено разделение прав на управление виртуальной инфраструктурой и на управление безопасностью. Для этого выделяются две основные роли: администратор виртуальной инфраструктуры и администратор информационной безопасности. Сервер авторизации vGate защищает периметр сети администрирования и разграничивает доступ серверам виртуализации и к средствам управления виртуальной инфраструктуры. Так же для улучшения отказоустойчивости в системе предусмотрел резервный сервер авторизации. При этом сеть администрирования отделяется от остальных сетей виртуальной инфраструктуры.

Ряд компонентов vGateразвертывается непосредственно на серверах виртуализации. Это требуется для обеспечения доверенной загрузки виртуальных машин и ряда других функций защиты.

Сеть виртуальных машин отделяется от остальных сетей виртуальной инфраструктуры. При необходимости сеть виртуальных машин может быть фрагментирована.

Данная технология позволяет на базе собственного оборудования университета развернуть безопасную облачную инфраструктуру, где можно реализовать задания, связанные с изучением информационных сетей и их защитой, а также с безопасностью хранения данных и т.д.

Примечания

1. Гузенкова Е.А. Верхорубова Н.А. Обеспечение оптимизации образовательного процесса за счет использования облачных технологий. / Перспективы развития информационных технологий: сборник материалов XVIII меж-дурар. науч.-практическ. конференции. – Новосибирск: ЦНРС, 2014. – С. 108-113.

2. Бирюков А. П. Безопасность -2014: облачная и мобильная. // ИнформКурьер-Связь – 2014. №10 (43). – С. 4-7.

3. Кусек К., Ван Ной В., Дэниел А. Администрирование VMwarevSphere 5: [пер. с англ.]. – СПб. : Питер, 2013. – 381 с.

Гузенкова Елена Алексеевна, ассистент кафедры «Информационные технологии и защита информации». Уральский государственный университет путей сообщения. E-mail:eguzenkova@usurt.ru

Гузенкова Елена Алексеевна, ассистент кафедры «Информационные технологии и защита информации». Уральский государственный университет путей сообщения. E-mail:eguzenkova@usurt.ru